Multi-Point Data Security Mechanism to Facilitate Secure Cloud Data Storage Solutions

Ansu Liz Thomas[a]
[a]Research Scholar,Department of Computer Science and Engineering, Noorul Islam Centre For Higher Education,kumaracoil
E-mail:[a*]lizansu@gmail.com

Abstract: Data security has repeatedly been a major issue for information technology. Because the data in the cloud computing environment is spread globally, this problem is very critical. Cloud computing offers protection against the two main reasons why users worry about their data's security and privacy. Even though numerous approaches to the problems of data security and privacy protection are becoming more crucial for the further development of cloud computing technology in business, industry, and government, Cloud computing has been studied in both academic and industrial settings. Data protection and security concerns affect cloud architecture, hardware, and software equally. This study aims to enhance data security and privacy protection for a dependable cloud environment by analyzing various security strategies and problems from both the software and hardware sides for securing data in the cloud. This essay explores a comparison of earlier studies on the methods used in cloud computing to protect the privacy and data security. A business can store data in the cloud rather than on-site using cloud storage, which is a type of cloud computing service. This method offers a workable substitute for keeping files on a third-party server and gives employees anytime, anywhere access to information.

Keywords: Data protection, Cloud computing, Cloud storage.

I. Introduction

The Internet is an open network technology and Nowadays it's a fundamental part of life. The service of the Internet is not limited to the user because of different types of network-based technologies in terms of data sharing. Data is shared from various resources more cheaply in the cloud, a new era of computer development technology. The cost is a vital thing of any organization where cloud ecosystem provides more benefit to the user or any organization is a low cost framework, pay-per-use model. Complicating matters, the MAS region's security concerns have not received the level of attention consistent with their in-depth academic research. To put it more bluntly, agent systems themselves are frequently insecure. Although it is not a new issue, security is now regarded as one of the most challenging ones. Network security has become a problem due to the ever-increasing scale, connectivity, and adoption of new information technologies. Many companies, organizations, and small businesses were driven to switch from standalone execution to cloud, edge, and fog paradigms by the desire to have a large storage capacity with practical scalability. Significantly, this transition presents a number of difficulties along the route. The idea entails a comprehensive management approach for personal data at the international data centers that house Edge, Fog, and Cloud. The sharing of enormous volumes of data and critical applications by cloud service providers with consumers has recently raised serious security and privacy concerns. In the study of computing paradigms, these concerns raise important questions about related themes. Each computer paradigm's current focus is on protecting users' privacy from intrusion by outsiders and fending off attacks. Additionally, maintaining data integrity is a crucial component, as is keeping it intact.

Several computing concepts are collectively referred to as "cloud computing," including the use of multiple PCs linked by an ongoing communication system (typically the Internet). Cloud computing is a linguistic word without a widely accepted, precise, specialized definition. The scientific term for distributed computing over a system is "cloud computing," which describes the capacity to run a program simultaneously on a significant number of connected PCs. The term's popularity can be attributed to the way it is used in advertising to promote facilitated benefits that operate customer server programming from a remote location. In a variety of attempts, a software agent system method has been used to provide security. The main goal of these systems was to address issues relating to specific security, like authorization and authentication. To maintain user information and data, data storage systems must be able to meet a number of challenging requirements, such as high availability, reliability, performance, replication, and data consistency. However, due to the inherent incompatibilities of the requirements, no single system can implement all of these requirements simultaneously. Security must be put in place at the data level to guarantee that business data is safe wherever it goes. Data security is a crucial component for managing cloud devices and maintaining their functionality. Data involved in transmissions or transfers must constantly be protected, and this may entail protection and restoration instructions for data and centres for cloud services.

Traditional healthcare systems currently use data processing and a centralized client-server architecture for patient health. Each healthcare facility still keeps data in silos, making it difficult to share information with other facilities for technological and logistical reasons due to infrastructure limitations. When a patient visits multiple hospitals, the absence of data sharing in a successful and secure data-sharing system results in resource and financial loss. In

general, there is a need for simple yet dependable procedures that offer a smooth learning process for storing enormous amounts of data. The majority of this research's attention is directed toward achieving cloud security and systems and safeguarding users' privacy from hackers. This research mainly focuses on how cloud security works. The cloud service provides certain data security requirements. If security flaws are to be minimized or completely eliminated, suppliers of cloud services have to adequately protect cloud-based client data. To ensure greater data security and include authentication procedures that restrict access to additional information, more potent data encryption techniques must be used. Access control through data encryption should be developed to make sure that only legitimately selected staff members to have access to the data.

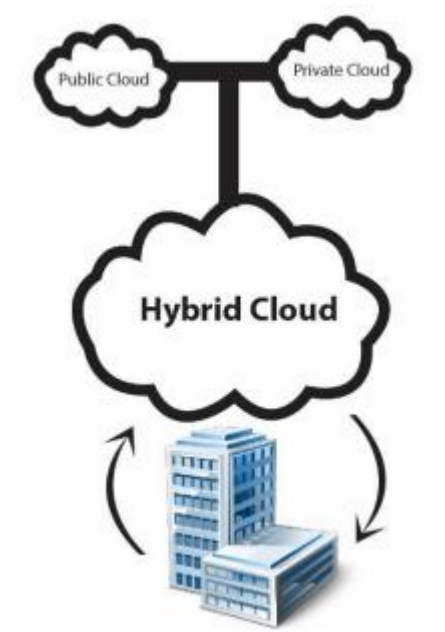

Figure 1: Different types of cloud computing technology

In the above Fig. 1. We show the various cloud computing platforms technology. In this paper, we use two security algorithms for data authentication purposes RSA data security algorithm and another is Elliptic curve cryptography. We are also user security socket layer (SSL) for data security purposes.

II. Analysis of review

After going through few related studies, there are numerous studies being conducted based on architecture of cloud based e learning and viewpoints of some papers are given below. To illustrate the proposed approach and give usage diagram in Fig. 2, this segment presents and examines situations that depend on reasonable contextual analyses to show the progression and conditions that must be considered for using the cloud security approach. The end user has no scope to access its own record and totally believe in its cloud service provider.

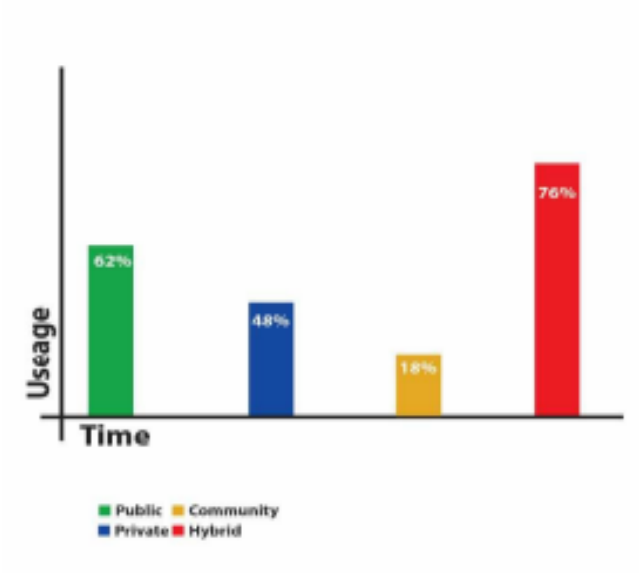

Figure 2. Use ages diagram of cloud services

From the review of different related papers on cloud-based learning security system, one can be aware of the benefit of using cloud base architecture and how it works. Present global technology is massively going toward cloud-based system to get an updated data security model. To conduct research based on above problem statement and objective, need to go with the comparison and analysis with different security aspects of multiple cloud based and how far they are user friendly in nature.

III. Need for cloud security

Despite the fact that there are fantastic alternatives for government agencies, the technology does carry some concerns. Many departments have been gradually switching to authorized cloud service providers ever since the Indian government started using the cloud. Because there is a wealth of relevant information in one place, CSPs are a common target for malicious activities. Government organizations must work with MSPs and CSPs, either directly or via their SIs, to safeguard their critical data and ensure that the necessary security precautions are taken. At the level of the data centre and cloud, a security fabric must be combined in addition to the regulations and compliances imposed by MeitY. Insider attacks are one issue that many CSPs are becoming worried about. The following list of security issues has been examined, including certain OWASP cloud security risks:

Figure 3. Cloud security concerns

IV. Cloud storage security challenges

- Operational Risks
- Data availability issues
- More data exposure
- Meeting compliance demands
- Cloud misconfigurations
- Inconsistent security controls

V. Methodology

A new technology called cloud computing may offer services quickly and cheaply. The three well-known and frequently used service models in the context of the cloud paradigm are infrastructures as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Clients of SaaS access the software and necessary data through web browsers thanks to a cloud service provider. In PaaS, a service provider offers users services through a collection of programs, each of which is equipped to carry out a particular task. To increase the productivity of their clients' businesses, IaaS providers give their clients access to storage and virtual machines.

Numerous applications of the cloud idea are based on services offered by service providers. Examples of well-known cloud applications supplied by vendors of cloud services, i.e., Google Apps Engine, Microsoft Azure, and Amazon Stack, are services provided by the Google, Microsoft, and Amazon enterprises. The ACME company also created a v-Cloud powered by VMware to make it easier for various businesses to share computing resources.

The three different types of clouds are public cloud, private cloud, and hybrid cloud, each with a different access scope. Public clouds are owned by service providers and available to the general public; private clouds are owned by businesses, and hybrid clouds combine public and private clouds. Presently, the majority of cloud service providers are well-known companies like Amazon, Google, and IBM. An exclusive cloud is one where only authorized users can access the services provided by the provider. Anyone can use cloud services, both public and private, in the public cloud, as opposed to an amalgamated cloud, which combines the concepts.

Security, management, and monitoring of resources are three of the main problems with cloud computing. There are currently no standards for control, and there are no established standards or criteria for deploying apps within a cloud. Although many cutting-edge techniques have been created and applied in the cloud, due to the unpredictability of the cloud environment, these techniques cannot completely guarantee security.

Discusses the fundamental problems with cloud computing management, governance, and data security [9]. The underlying security, privacy, and trust issues in the context of modern cloud computing were highlighted by Sun et al. [10], who also gave instructions to users on how to recognize both overt and covert risks related to its use. According to the authors, security, privacy, and trust are the three main potential risks associated with cloud computing. The idea of computing as a utility has finally materialized, and security is now crucial. It has four subcategories that can be separated out: security features, data privacy, cloud server tracking or monitoring; and preventing criminal insiders from committing evil deeds and service snatching.

Networks for cloud computing are intended to have a data security framework [11]. The writers mostly covered security concerns with cloud data storage. Additionally, several data storage security solutions are covered by patents [12]. Younis and Kifayat offer a survey of secure cloud computing for critical infrastructure [13]. For the integration of RFID technology with cloud computing and the Internet of Things, a security and privacy architecture has been put forth [14].

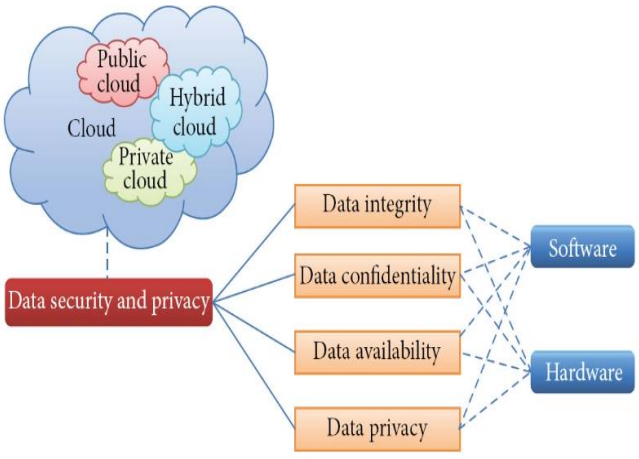

Figure 4. Organization of data security and privacy in cloud computing

In this essay, we'll look at a number of security methods as well as concerns about safeguarding data privacy and security in a cloud computing environment. Figure 1 provides an illustration of how this work compares and evaluates earlier research on cloud computing solutions using data security issues like data integrity, confidentiality,

and availability. Because data security and privacy are frequently linked, cloud technologies and data privacy issues are also examined. Comparative studies on data security and privacy may help to boost consumer confidence by protecting data in the cloud computing environment.

VI. Data integrity

Data integrity is one of the most important elements of any information system. The general definition of data integrity is safeguarding information from unauthorized addition, deletion, modification, or fabrication. Managed entity access and rights to particular company resources help prevent the misuse, exploitation, and theft of priceless information and services.

Data integrity is easily attained in a standalone system with a single database. Through database constraints and transactions, which are normally handled by a database management system, data integrity is assured in the standalone system (DBMS). Transactions must follow the ACID (atomicity, consistency, isolation, and durability) requirements in order to ensure data integrity. Most databases are capable of handling ACID transactions and maintaining data integrity.

VII. Data confidentiality

Data confidentiality is essential if consumers are to keep their personal or sensitive data in the cloud. Access control and authentication procedures are used to ensure that. The issues with data confidentiality, authentication, and access control in cloud computing may be solved by enhancing cloud reliability and trustworthiness.

Due to the lack of user trust in cloud service providers and the near impossibility of them preventing internal threats, customers should avoid storing sensitive data directly in the cloud. Simple encryption cannot satisfy complex requirements like inquiry, concurrent change, and fine-grained authorization due to key management issues.

VIII. Data availability

Data availability describes the extent to which how a user can independently check their data rather than depending entirely on the credit guarantee of the cloud service provider, as well as how their data can be accessed or recovered in the event of a disaster, such as hard disk damage, an IDC fire, or a network outage

Clients have serious concerns about data storage on international servers because cloud providers are constrained by regional laws, and cloud users should be aware of these limitations. The cloud service provider must also provide data security, including data integrity and confidentiality. All of these concerns should be discussed with the client by the cloud service provider in order to build a trusting relationship. The cloud provider should reassure customers about the security of their data and explain how local laws will be applied. The study mainly concentrates on data problems and challenges related to price, availability, and security, as well as the location and relocation of data storage.

IX. Data privacy

Privacy is the ability to keep one's identity or personal information a secret and only disclose it when required. The following are the components of privacy.

i. When: A topic may be more concerned with information about the present or the future than information about the past.
ii. How: A user might feel fine with friends being able to directly request their information, but they might not want notifications being sent out regularly and automatically.
iii. Extent: Rather than receiving a precise point of information, a user can prefer to get an ambiguous region.

X. Cloud security design principles

1. Security at all layers: Make sure that their design is applied with numerous security measures at all layers (physical, network, data, application, etc.). This will provide complete protection of the applications and data that departments host on the cloud-based platform
2. Protect data during transmission and at rest: Determine the data's criticality and sensitivity levels and classify it accordingly. By utilising the security mechanisms that are already in place, such as access control, tokenization, encryption, etc., this can be avoided.
3. Monitoring and auditing: Ensure that alerting, auditing, and monitoring are configured to quickly identify system changes. Log integration and metric gathering can also automatically examine, act, and respond.
4. Controls for managing access: Ensure that the principle of selected privileges is applied and impose the separation of duties with the proper access and authorisation. Any unwanted access and information loss/theft can be stopped via centralised identity and access control.
5. Security event readiness: The department and CSP must set up the system for any unusual security occurrence. To find the security flaws and problems, regular vulnerability and security testing must be performed. To keep track of how the Cloud systems respond at different layers, several drills can be carried out.
6. Automate security best practices by using AI, ML, and bots to automate software, hardware, and application-based security systems. This will increase the security of the environment by enabling regular checks and the implementation of the controls required to thwart attacks and improve cloud security.
7. Since there are no common standards among it becomes difficult to move data from one cloud provider to another or to an on-premise Data centre because there are so many distinct cloud providers for data exports and migration. The prevention of vendor lock-in by cloud service providers while

hosting the application or data is the responsibility of the relevant departments.

XI. Performance evaluation metrics

The suggested approach is examined using performance evaluation measures. The following metrics were applied.

1. Reaction Time
2. Message Encryption
3. IAES Encryption time
4. IAES decryption time
5. Total IAES time
6. MRSA Encryption time
7. MRSA decryption time
8. Total MRSA time
9. Total time

XII. Conclusion

Governments and organizations are increasingly moving workloads to the cloud. Due to persisting worries about data security in cloud computing, some firms are still reluctant to take advantage of the cloud's many benefits. In the cloud ecosystem provides service to end-users by providing security to the sensitive data from spiteful user. Hybrid cloud provide a distinct security solution for the level of information management. The service based on cloud infrastructure platform oriented to ensure that reliable, the data must be protected using different kind of algorithm and evaluation has to be taken place in cloud-based security system. This research is to minimize the risk factor after analysing the different cloud based architectural model of different educational institutes. There will be also a cost bandwidth factor analysis with user friendly approach of the proposed secured architectural model.

References

[1] Tang, Jianhang, Mohammad Mussadiq Jalalzai, Chen Feng, Zehui Xiong, and Yang Zhang. "Latency-Aware Task Scheduling in Software-Defined Edge and Cloud Computing with Erasure-Coded Storage Systems." *IEEE Transactions on Cloud Computing* (2022).

[2] ThiBac, Do, and Nguyen Hieu Minh. "Design of network security storage system based on under cloud computing technology." *Computers and Electrical Engineering* 103 (2022): 108334.

[3] Seth, Bijeta, Surjeet Dalal, Vivek Jaglan, Dac-Nhuong Le, Senthilkumar Mohan, and Gautam Srivastava. "Integrating encryption techniques for secure data storage in the cloud." *Transactions on Emerging Telecommunications Technologies* 33, no. 4 (2022): e4108.

[4] Mast, Kai, Andrea C. Arpaci-Dusseau, and Remzi H. Arpaci-Dusseau. "LambdaObjects: Re-aggregating storage and execution for cloud computing." In *Proceedings of the 14th ACM Workshop on Hot Topics in Storage and File Systems*, pp. 15-22. 2022.

[5] Kaliyamoorthy, Priyadharshini, and Aroul Canessane Ramalingam. "QMLFD Based RSA Cryptosystem for Enhancing Data Security in Public Cloud Storage System." *Wireless Personal Communications* 122, no. 1 (2022): 755-782.

[6] Fu, Jun-Song, Yun Liu, Han-Chieh Chao, Bharat K. Bhargava, and Zhen-Jiang Zhang. "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing." *IEEE Transactions on Industrial Informatics* 14, no. 10 (2018): 4519-4528.

[7] Mutlag, Ammar Awad, Mohd Khanapi Abd Ghani, Net al Arunkumar, Mazin Abed Mohammed, and Othman Mohd. "Enabling technologies for fog computing in healthcare IoT systems." *Future Generation Computer Systems* 90 (2019): 62-78.

[8] Sajid, Faiqa, Muhammad Abul Hassan, Ayaz Ali Khan, Muhammad Rizwan, Natalia Kryvinska, Karovič Vincent, and Inam Ullah Khan. "Secure and Efficient Data Storage Operations by Using Intelligent Classification Technique and RSA Algorithm in IoT-Based Cloud Computing." *Scientific Programming* 2022 (2022).

[9] Asesh, Aishwarya. "Encryption technique for a trusted cloud computing environment." *IOSR J Comput Eng* 17, no. 1 (2015): 53-60.

[10] Xu, Zhiyan, Libing Wu, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, and Debiao He. "A secure and efficient public auditing scheme using RSA algorithm for cloud storage." *The Journal of Supercomputing* 73, no. 12 (2017): 5285-5309.

[11] Mukhopadhyay, Bholanath, Rajesh Bose, and Sandip Roy. "A novel approach to load balancing and cloud computing security using SSL in IaaS environment." *International Journal* 9, no. 2 (2020).

[12] Kumar, Y. Kiran, and R. Mahammad Shafi. "An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem." *International Journal of Electrical and Computer Engineering* 10, no. 1 (2020): 530.

[13] Farsi, Mohammed, Munwar Ali, Reehan Ali Shah, Asif Ali Wagan, and Radwan Kharabsheh. "Cloud computing and data security threats taxonomy: A review." *Journal of Intelligent & Fuzzy Systems* 38, no. 3 (2020): 2517-2527.

[14] Gandhi, Kanika S., Devashree S. Patekar, Garima M. Virulkar, Kulshree S. Damle, DurveshSingh Thakur, and Ms Shwetambari G. Pundkar. "Secure Encrypted Data Deduplication using Hashing Technique in Cloud." (2020).

[15] Deng, Hua, Zheng Qin, Qianhong Wu, Zhenyu Guan, Robert H. Deng, Yujue Wang, and Yunya Zhou. "Identity-based encryption transformation for flexible sharing of encrypted data in public cloud." *IEEE Transactions on Information Forensics and Security* 15 (2020): 3168-3180.

[16] Shen, Jian, Dengzhi Liu, Xingming Sun, Fushan Wei, and Yang Xiang. "Efficient cloud-aided verifiable secret sharing scheme with batch verification for smart cities." *Future Generation Computer Systems* 109 (2020): 450-456.

[17] A Almusaylim, Zahrah, and N. Z. Jhanjhi. "Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing." *Wireless Personal Communications* 111, no. 1 (2020): 541-564.

[18] B. Karthikeyan, T. Sasikala, and S. Baghavathi Priya. "Key exchange techniques based on secured energy efficiency in mobile cloud computing." *Applied Mathematics & Information Sciences* 13, no. 6 (2019): 1039-1045.

.